Update on DNSSEC for the Root Zone

NANOG 49, June 14, 2010
ISP Security Track

Duane Wessels
VeriSign
The DURZ

- The 13 Root Servers were incrementally converted to a signed, but unvalidatable, zone beginning in January and finishing in May.
- Root Server operators collaborated with DNS-OARC to collect DNS queries 24 hours before and after each switchover.
DURZ Data Analysis

• Looking at the data for indications of problems
• Query Rates
• TCP traffic
• Message sizes
• Priming queries
J-root
On Its Own

UDP Query Rate

Queries Per Second

Apr14 Apr15 Apr16
13 17 21 01 05 09 13 17 21 01 05 09 13 17 21

J
H DURZ
C DURZ
G DURZ
B DURZ
F DURZ
TCP Query Rate

This drop is due to upgraded resolvers within an ISPs /23.
DNS Message Sizes
For J-root

Mean Size, Bytes

Responses
Queries
UDP Priming Query Rate for the previous month as of 2010-05-01 00:00:00

A single Cisco CNR instance with max-cache-ttl=0
KSK Generation

• First KSK ceremony takes place in two days.
• Somewhere on the U.S. East coast, outside the nuclear blast zone of Washington, DC.
• ICANN staff plus 14 Trusted Community Representatives acting as Crypto Officers and Recovery Key Share Holders.
• Expected to take about 6 hours.
• Key material then replicated and stored in the West coast facility.
DVRZ

- A fully validatable Root Zone is currently planned to be published on July 15.
- Another 48-hour data collection.
- Root Zone trust anchor to be published by ICANN (the IANA functions operator).
Acknowledgements

Bringing DNSSEC to the Root Zone is a result of cooperation between ICANN & VeriSign with support from the U.S. DoC NTIA and NIST

Joe Abley
Mehmet Akcin
David Blacka
David Conrad
Richard Lamb
Matt Larson

Fredrik Ljunggren
Dave Knight
Tomofumi Okubo
Jakob Schlyter
Duane Wessels

http://www.root-dnssec.org